REMARKS

The Official Action mailed September 18, 2008 has been carefully considered. Claim 16 was amended to more positively recite method steps in the claim. Applicants respectfully submit that the scope of this claim has not been changed that would require a further search. No new matter has been added to the subject application as a result of the changes made thereto. Reconsideration and allowance of the subject application, as amended, are respectfully requested.

Discussion of rejections of claims 1-3, 9 and 10 under §103(a)

Claims 1-3, 9 and 10 stand rejected under §103(a) as being obvious over Vairavan in view of Hui et al, Canion et al, Foschiano et al, and Yang et al. As to claims 1 and 9, the Examiner alleges that Variavan discloses at least one wide area network (WAN); at least one local area network (LAN); and an integrated firewall/VPN chipset configured to send and receive data packets between said WAN and said LAN. The Examiner also points to Vairavan as teaching filtering techniques within different firewall layers, a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a content match packet filtering engine configured to analyze the scope of at least one data packet. The Examiner relies on Hui as teaching a firewall which provides packet filtering function along with application proxy function, i.e. a third layer including at least one application proxy configured to provide additional pattern matching. Further, the Examiner asserts that Hui teaches a listening table which stores a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking.

The Examiner relies on Canion for teaching a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking. The Examiner relies on Foschiano as teaching a hardware engine to provide pre-analysis processing to reduce the workload of a CPU. Also, according to the Examiner, Variavan discloses a VPN configured to provide security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, and decapsulation of said data packets; an interface configured to determine if said data packets are plain text or cipher text, said

interface further configured to forward a preselected number of bytes to said firewall if said data packet are plain text, said interface further configured to forward said data packets to said VPN if said data packets are cipher text. Further, Vairavan teaches a VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further includes an inbound security database having database of tunnels configured to provide VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having marocodes configured to instruct said VPN processor to decrypt and decapsulate said at least one data packet according to a user-defined security procedure. Also, Yang teaches the VPN including a VPN packet buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to provide VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet.

To give a better understanding to the scope and of claims 1 and 9 and clarify the differences between claims 1 and 9 of the claimed invention and cited references, the applicant respectfully presents claims 1 and 9 of the claimed invention as follows:

> 1. An integrated firewall/VPN system, comprising:
>
> at least one wide area network (WAN);
>
> at least one local area network (LAN);
>
> at integrated firewall/VPN chipset configured to send and receive data packets between said WAN and said LAN, said chipset comprising:
>
> a firewall comprising a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of at least one data packet, a third layer including at least one application proxy configured to provide additional pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) and a fourth layer including a session match engine configured to

store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking;

a VPN configured to provide security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, and decapsulation of said data packets, said VPN including a VPN packet buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to provide said inbound VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having microcodes configured to instruct said VPN processor to decrypt and decapsulate said at least one data packet according to a user-defined security procedure; and

an interface configured to determine if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packets are plain text, said interface further configured to forward said data packets to said VPN if said data packets are cipher text.

9. A firewall/VPN integrated circuit ({IC}, comprising:

a router core configured to interface between at least one untrusted network and at least one trusted network to send and receive data packets between said untrusted and said trusted networks;

a firewall system, comprising a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of at least one data packet, a third layer including at least one application proxy configured to provide additional pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) and a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking;

a VPN configured to provide security functions for data between said at least one untrusted and said at least one trusted metwork, wherein said security functions comprise encryption, decryption, encapsulation, and decapsulation of said data packets, said VPN including a VPN packet

> buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to provide said inbound VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having microcodes configured to instruct said VPN processor to decrypt and decapsulate said at least one data packet according to a user-defined security procedure; and
>
> an interface configured to determine if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packets are plain text, said interface further configured to forward said data packets to said VPN if said data packets are cipher text.

First of all, according to the claimed invention, the firewall includes a session match engine configured to store a TCP/UDP connection setup in a look-up table and to forward the setup progress to said CPU for tracking. The inventive session match engine is configured to keep the TCP/UDP connection setup in an embedded look-up table and catch control messages (e.g., 3-way handshaking messages) during the TCP/UDP connection setup. The session match engine is further configured to forward the control messages to the general CPU for tracking the setup progress. Hui is understood to disclose a policy engine module configured to set up the TCP/UDP connection parameters in a listening table and establish network connection with external network devices. However, the policy engine module of Hui does not appear configured to forward the network setup progress to CPU for tracking. Furthermore, Canion only appears to teach that an internal protocol may be provided and implemented as a set of messages exchanged across the switch fabric. These messages indicate the arrival of new inbound or outbound packet on existing connections, along with identifiers or tags for those connections. However, these messages are used internally for notifying the advent of coming packets on existing connection, but are not control messages for tracking the progress of a TCP/UDP connection. Hence, neither Hui or Canion appear to disclose a session match engine configured to forward the TCP/UDP connection setup progress, e.g.,. the 3-way handshaking control messages, to the CPU for

tracking. The Applicant respectfully calls the Examiner's attentions to the difference between the session match engine of Hui and Canion and the session match engine of the claimed invention in this regard.

Secondly, according to the claimed invention, the firewall/VPN integrated chipset includes an interface configured to scrutinize the received data packets to see if the received data packets are plain text or cipher text. The inventive interface is further configured to forward a preselected number of bytes to the firewall if the data packets are plain text and forward the data packets to VPN if the data packets are cipher text. The Examiner alleges that Vairavan discloses an interface configured to determine if data packets are plain text or cipher text, the interface further configured to forward a preselected number of bytes to the firewall if the data packet are plain text, the interface further configured to forward the data packets to the VPN if the data packets are cipher text.

However, Applicant disagrees with the Examiner's characterization of Vairavan. In contrast to the Examiner's assertions, the interface of Vairavan does not have the same configuration as the interface of the claimed invention. Vairavan discloses a method for routing data packets received from an access interface. According to Vairavan, the interface is configured to receive the incoming data packets and the packet processor is configured to determine if the received data packets is a VPN packet or a wireless packet. If the data packet is determined to be a VPN packet, the packet is processed by the packet processor and/or the security processor by a series of processing steps, including decryption, error checking, reassembling, and firewall filtering, as shown in Fig. 7 of Vairavan. If the data packet is determined to be a wireless packet, the packet is processed by the packet processor and/or the security processor by a series of processing steps, including security check, authorized connection check, data compression, and firewall filtering, as shown in Fig. 8 of Vairavan.

Thus, **the interface of Vairavan is not configured to determine the type of incoming data packets.** Besides, **the interface of Vairavan is configured to forward both the VPN packets and the wireless packets to the same module, i.e. the packet processor and/or security processor, whereas the interface of the claimed invention is configured to forward the VPN data packet and firewall data packet respectively to different modules, i.e. the**

VPN module and the firewall module. Also, **the interface of Vairavan is not configured to forward the incoming data packets to different modules according to the type of the incoming data packets.** Further, **the interface of Vairavan is not configured to forward a preselected number of bytes to the firewall if the data packets are plain text.** These manifestations are sufficient to demonstrate that the interface of Vairavan has a different configuration and functionality with the interface of the claimed invention. The Applicant respectfully calls the Examiner's attentions to the difference between the interface of Vairavan and the interface of the claimed invention in these regards.

In brief, claims 1 and 9 of the claimed invention is distinguishable from the combination of the cited references in terms of the following respects: (1) The firewall system of the claimed invention includes a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to the CPU for tracking, whereas both Hui and Canion do not disclose a session match engine capable of forwarding the TCP/UDP connection setup progress to the CPU for tracking; and (2) The claimed invention includes an interface configured to determine the type of incoming data packets and route the incoming data packets to different modules for processing according to the type of the data packets, in which if the data packets are plain text, a preselected number of bytes is routed to the firewall The interface of Vairavan is configured to receive the data packets only. The interface of Vairavan is not configured to determine the type of incoming data packets and route the incoming data packets to different modules for processing according to the type of the data packets. Also, the interface of Vairavan is not configured to route a preselected number of bytes to firewall if the incoming data packets are plain text.

Accordingly, it is respectfully submitted that no combination of the cited references couyld achieve or render obvious Applicant's claimed inventions. Moreover, it is respectfully submitted that one skilled in the art would not make the combination suggested by the Examiner because this combination would not arrive at the claimed invention. Thus, claims 1 and 9 should be patentable over the cited references either alone or in combination.

Furthermore, since the independent claims 1 and 9 are patentable over these cited references, claims 2, 3 and 10 should also be allowable due to their dependency with their base

claims. Hence, the applicant respectfully submits that claims 2, 3 and 10 should also be patentable over these cited references.

Discussion of rejections of claims 4 and 11 under §103(a)

As per the Examiner, claims 4 and 11 are rejected under §103(a) as being obvious over Vairavan in view of Hui et al, Canion et al, Foschiano et al, Yang et al and Lee. The deficiencies of Vairavan, Hui et al, Canion et al, Foschiano et al and Yang et al are discussed above in reference to claims 1 and 9. It is not seen how Lee supplies the missing teachings to these references to render obvious claims 1 and 9, nor is Lee being cited as providing such teachings. Since the independent claims 1 and 9 are patentable, claims 4 and 11 should also be allowable due to their dependency with their base claims. Hence, the Applicant respectfully submits that claims 4 and 11 should also be patentable over the cited references.

Discussion of rejections of claims 5, 6, 12 and 13 under §103(a)

As per the Examiner, claims 5, 6, 12 and 13 are rejected under §103(a) as being obvious over Vairavan in view of Hui et al, Canion et al, Foschiano et al, Yang et al and Krishna et al. Since the independent claims 1 and 9 are patentable, claims 5, 6, 12 and 13 should also be allowable due to their dependency with their base claims. Hence, the applicant respectfully submits that claims 5, 6, 12 and 13 should also be patentable over the cited references.

Discussion of rejections of claims 8, 15 and 16 under §103(a)

As per the Examiner, claims 8, 15 and 16 are rejected under §103(a) as being obvious over Vairavan in view of Hui et al, Canion et al, Foschiano et al, Yang et al and Osborne et al. As to claim 16, the Examiner alleges that Vairavan discloses a filtering technique within different firewall layers, a first layer including a header match packet filtering engine, a second layer including a content match packet filtering engine configured to analyze the scope of at least one data packet. Vairavan further discloses a VPN configured to provide security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, decapsulation of said data packets; an interface configured to determine if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packets are plain text, said interface further configured to forward said data packets to said VPN if said

data packets are cipher text. Further, Vairavan teaches a VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further includes an inbound security database having database of tunnels configured to provide VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having macrocodes configured to instruct said VPN processor to decrypt and decapsulate said at least one data packet according to a user-defined security procedure. Also, Hui teaches a firewall which provides packet filtering function along with application proxy function, a third layer including at least one application proxy configured to provide additional pattern matching. Further, Hui teaches a listening table which stores a TCP/UDP connection setup and to forward the setup progress to a central processing unit (CPU) for tracking. Further, Canion teaches a fourth layer including a session match engine configured to store a TCP/UDP connection setup and to forward the setup progress to a central processing unit (CPU) for tracking. Also, Foschiano teaches hardware engine to provide pre-analysis processing to reduce the workload of a central processing unit (CPU). Also, Yang teaches a VPN including a VPN packet buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to provide VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet. Further, Osborne teaches a method of processing a data packet comprising the steps of: defining one or more access control protocols; receiving a data packet; selecting a certain number of bytes of said data packet; and processing said selected bytes using said access control protocols.

However, it is to be noted that the method of operation according to claim 16 is different from the combination of the cited references in terms of packet routing. As stated above, Vairavan fails to disclose the method of forwarding different types of data packets, i.e. the VPN packets which are cipher text and the wireless packets which are plain text respectively to different modules, i.e. the firewall module and the VPN module. Osborne discloses a process for demultiplexing encapsulated data segments, e.g. IP datagram, TCP segment, and UDP segment. According to Osborne, the encapsulated data segments are categorized and dispatched to be

processed by appropriate network layer protocol. However, these encapsulated data segments are of the same type, i.e. Ethernet data packet, and they are all plain text. Hence, Osborne fails to suggest the method of forwarding different types of data packets, i.e. the VPN packets which are cipher text and the wireless packets which are plain text respectively to different modules, i.e. the firewall module and the VPN module. It can be readily known to an artisan skilled in the art that even if the cited references are combined, the combination thereof can not suggest the method of routing data packets of different types, i.e. VPN packets which are cipher text and Ethernet packets which are plain text, respectively to appropriate modules for processing. The applicant respectfully submits that the process of claim 16 of the claimed invention can not be suggested or taught by the cited references, and claim 16 should be patentable over the cited reference in this respect.

In order to clarify the difference between the method of operation disclosed by the claimed invention and the cited references, the applicant amended claim 16 to reflect such difference. The applicant respectfully submits that the amendments made to claim 16 is supported by the original specification, and no new matter has been entered in virtue of the amendments. It is believed that the rejection to claim 16 is obviated.

Furthermore, since the independent claims 1 and 9 are patentable, claims 8 and 15 should also be allowable due to their dependency with their base claims. Hence, the applicant respectfully submits that claims 8 and 15 should also be patentable over the cited references.

For the foregoing reasons, it is believed that claims 1-6, 8-13, 15, 16 are allowable. The applicant respectfully submits that the claimed invention is patentable over the cited references either alone or in combination, and reconsideration and allowance of the present patent application are earnestly solicited at an early date

Having dealt with all the objections raised by the Examiner, it is respectfully submitted that the present application, as amended, is in condition for allowance. Thus, early allowance is earnestly solicited.

If the Examiner desires personal contact for further disposition of this case, the Examiner is invited to call the undersigned Attorney at 603.668.6560.

In the event there are any fees due, please charge them to our Deposit Account No. 50-2121.

Respectfully submitted,

By: /Edmund P. Pfleger/
Edmund P. Pfleger
Reg. No. 41252